AMENDMENTS TO THE CLAIMS

Please cancel claim 26 without prejudice. Kindly amend claims 1, 8, 16, 18, 23, 25, and 27-29 as shown in the following listing of claims. The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

a microprocessor;

a control word, configured to prescribe one of a plurality of data block sizes to be employed during execution of one of the cryptographic operations, wherein said control word is stored in memory, and wherein a memory location of said control word is prescribed by contents of a register that is referenced by a single atomic cryptographic instruction;

fetch logic, disposed within ~~a microprocessor~~said microprocessor, configured to receive ~~a single~~said single atomic cryptographic instruction as part of an instruction flow executing on said microprocessor, wherein said single atomic cryptographic instruction ~~prescribes~~ prescribes said one of the cryptographic operations, and wherein said single atomic cryptographic instruction ~~prescribes one of a plurality of data block sizes~~references said control word;

translation logic, coupled to said fetch logic, configured to translate said single atomic cryptographic instruction into a sequence of micro instructions that directs said microprocessor to perform said one of the cryptographic operations; and

execution logic, disposed within said microprocessor and operatively coupled to said single atomic cryptographic instruction, configured to execute said one of the cryptographic operations, said execution logic comprising:

a cryptography unit, configured ~~to execute~~ to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said one of a plurality of data block sizes ~~is prescribed by a control word that~~ is provided to a block size controller within said cryptography unit, wherein said block size controller employs said one of a plurality of data block sizes during execution of said one of the cryptographic operations.

2. (Original) The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

3. (Original) The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

4. (Original) The apparatus as recited in claim 1, wherein said one of a plurality of data block sizes comprises 128 bits.

5. (Original) The apparatus as recited in claim 1, wherein said one of a plurality of data block sizes comprises 192 bits.

6. (Original) The apparatus as recited in claim 1, wherein said one of a plurality of data block sizes comprises 256 bits.

7. (Original) The apparatus as recited in claim 1, wherein said one of the cryptographic operations is executed according to the Advanced Encryption Standard (AES) algorithm.

8. (Currently Amended) The apparatus as recited in claim 1, wherein said ~~data blockblock size~~ controller is configured to interpret a data block size field within ~~a control~~said control word which is referenced by said single atomic cryptographic instruction.

9. (Previously Presented) The apparatus as recited in claim 1, wherein said single atomic cryptographic instruction is prescribed according to the instruction format for execution on an x86-compatible microprocessor.

10. (Previously Presented) The apparatus as recited in claim 1, wherein said single atomic cryptographic instruction implicitly references a plurality of registers within said microprocessor.

11. (Original) The apparatus as recited in claim 10 wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of a plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished, said plurality of input text blocks are sized according to said one of a plurality of data block sizes.

12. (Original) The apparatus as recited in claim 10, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks, wherein said plurality of input and output text blocks are sized according to said one of a plurality of data block sizes.

13. (Previously Presented) The apparatus as recited in claim 10, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of blocks within a plurality of input text blocks, wherein said plurality of input text blocks are sized according to said one of a plurality of data block sizes.

14. (Original) The apparatus as recited in claim 10, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

15. (Original) The apparatus as recited in claim 10, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations.

16. (Currently Amended) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a ~~sixth~~said register, wherein contents of ~~said sixth register~~said register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying ~~a fifth location in memory~~said memory location for access of ~~a control~~said control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations, and wherein said control word comprises:

a data block size field, configured to specify said one of a plurality of data block sizes to be employed during execution of said one of the cryptographic operations.

17. (Cancelled)

18. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

a microprocessor;

a control word, configured to prescribe a block size to be employed during execution of one of the cryptographic operations, wherein said control word is stored in memory, and wherein a memory location of said control word is prescribed by contents of a register that is referenced by a single atomic cryptographic instruction;

a cryptography unit disposed within execution logic in ~~a microprocessor~~ said microprocessor, configured to execute ~~one of~~ said one of the cryptographic operations responsive to receipt by said microprocessor of ~~a single~~ said single atomic cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said single atomic cryptographic instruction is fetched from memory by fetch logic in said microprocessor, ~~and wherein said single atomic cryptographic instruction also prescribes a block size to be employed when executing said one of the cryptographic operations,~~ and wherein translation logic in said microprocessor translates said single atomic cryptographic instruction into a sequence of micro instructions that directs said microprocessor to perform said one of the cryptographic operations; and

block size logic, operatively coupled within said cryptography unit, configured to direct said microprocessor to employ said block size when performing said one of the cryptographic operations.

19. (Original) The apparatus as recited in claim 18, wherein said block size comprises 128-bits.

20. (Original) The apparatus as recited in claim 18, wherein said block size comprises 192-bits.

21. (Original) The apparatus as recited in claim 18, wherein said block size comprises 256-bits.

22. (Original) The apparatus as recited in claim 18, wherein said one of the cryptographic operations is executed according to the Advanced Encryption Standard (AES) algorithm.

23. (Currently Amended) The apparatus as recited in claim 18, wherein said block size logic is configured to interpret a data block size field within ~~a control~~said control word which is referenced by said single atomic cryptographic instruction.

24. (Previously Presented) The apparatus as recited in claim 18, wherein said single atomic cryptographic instruction is prescribed according to the instruction format for execution on an x86-compatible microprocessor.

25. (Currently Amended) A method for performing cryptographic operations in a device, the method comprising:

via fetch logic within a microprocessor, fetching a single atomic cryptographic instruction from memory that prescribes ~~employment of particular data block size during execution of~~ one of a plurality of cryptographic operations, and via translation logic disposed within the microprocessor, translating the single atomic cryptographic instruction into a sequence of micro instructions that direct the microprocessor to perform the one of the plurality of cryptographic ~~operations; andoperations;~~

via a field within a control word that is referenced by the single atomic cryptographic instruction, specifying a particular data block size to be employed during execution of the one of a plurality of cryptographic operations, and

via a cryptography unit disposed within execution logic in the ~~microprocessor~~ microprocessor, employing the particular data block size when performing the one of the cryptographic operations.

26. (Cancelled)

27. (Currently Amended) The method as recited in ~~claim 26~~claim 25, wherein said specifying comprises:

prescribing 128 bits as the particular block size.

28. (Currently Amended) The method as recited in ~~claim 26~~claim 25, wherein said specifying comprises:

prescribing 192 bits as the particular block size.

29. (Currently Amended) The method as recited in ~~claim 26~~claim 25, wherein said specifying comprises:

prescribing 256 bits as the particular block size.

30. (Original) The method as recited in claim 25, wherein said employing comprises:

executing the one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm.

31. (Previously Presented) The method as recited in claim 25, wherein said fetching comprises:

prescribing the single atomic cryptographic instruction according to the instruction format for execution on an x86-compatible microprocessor.